(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 085 605 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.04.2025 Bulletin 2025/18

(21) Application number: **20908633.9**

(22) Date of filing: **09.12.2020**

(51) International Patent Classification (IPC):
H04M 3/436 *(2006.01)* ***H04M 3/42*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
H04M 3/436; H04M 3/42059; H04M 2203/551; H04M 2203/558; H04M 2203/6027; H04M 2203/6045

(86) International application number:
PCT/US2020/063879

(87) International publication number:
WO 2021/138007 (08.07.2021 Gazette 2021/27)

(54) DYNAMICALLY PROVIDING SAFE PHONE NUMBERS FOR RESPONDING TO INBOUND COMMUNICATIONS

DYNAMISCHE BEREITSTELLUNG VON SICHEREN TELEFONNUMMERN ZUM BEANTWORTEN EINGEHENDER KOMMUNIKATION

FOURNITURE DYNAMIQUE DE NUMÉROS DE TÉLÉPHONE SANS DANGER POUR RÉPONDRE À DES COMMUNICATIONS ENTRANTES

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **31.12.2019 US 201916731715**
21.10.2020 US 202017075846

(43) Date of publication of application:
09.11.2022 Bulletin 2022/45

(73) Proprietor: **Youmail, Inc**
Irvine, CA 92606 (US)

(72) Inventors:
- **QUILICI, Alexander, E.**
  Malibu, CA 90265 (US)
- **RUDOLPH, Michael, J.**
  San Juan Capistrano, CA 92675 (US)

(74) Representative: **Guardian IP Consulting I/S**
Diplomvej, Building 381
2800 Kgs. Lyngby (DK)

(56) References cited:
US-A1- 2012 287 823
US-A1- 2012 287 823
US-A1- 2015 023 485
US-A1- 2015 121 480
US-A1- 2018 249 006
US-A1- 2020 053 205
US-B1- 9 060 057

EP 4 085 605 B1

Description

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] This application generally relates to scanning messages for fraud, and in particular, evaluating whether contact information in messages are associated with legitimate entities and substituting proper contact information before a user attempts to return the message.

DESCRIPTION OF THE RELATED ART

[0002] Currently, a "robocaller," telemarketer, or scammer can disseminate a phone number or other contact information by means of communication via a call, text, or email. If the communication is not blocked, the communicator may leave a message, such as a voice message, with a phone number or contact information that the recipient of the communication should call back. The message may suggest that the phone number or contact information is, for example, the recipient's bank, car company, credit card, the IRS (Internal Revenue Service) or other government entity, and may state that the user is required to return the call because of an alleged fraud on their account or an expiring warranty or other urgent need. The message may use a reputable name, such as a name of a bank, credit card company, or other business name to give an authentic appearance.

[0003] When the recipient returns the call or communication, however, they are solicited or scammed into buying a service they don't need, prompted to provide account information which can result in identity theft, or otherwise inconvenienced or harmed by virtue of having contacted an entity with which they do not wish to communicate. Many smartphones currently facilitate a user returning a call to this improper phone number by generating a link on the phone number in the transcribed voice message, text message or email that the user merely needs to touch to then be taken to a phone app with the number loaded into the dial field ready to be called. Current voicemail or inbox systems do not assist communication recipients in distinguishing contact from fraudulent or other untrustworthy entities from legitimate entities.

[0004] As a result, if a recipient wants to somehow determine whether the given entity that appears to have contacted them is "real", they need to do time-consuming real-time research - for example, an internet search - to look up the official contact information from the entity, such as on their web site or "contact us" page, which itself may encounter fake information (due to incorrectly entered web site names or fraudulent search results).

[0005] Patent application US 2018/249006 discloses a system operable to receive an automated call from a communications device, determine whether preferences associated with a called party identity is applicable to the automated call, and determine whether a condition that precludes acceptance of the automated call is present (where the determination of whether the condition is present can be based on information received from a sensory device coupled to the user device). In response to the condition being determined to be present, the automated call can be denied.

[0006] There is thus a need for a message scanning system that can authenticate contact information of legitimate entities to prevent users from returning calls to untrustworthy or improper phone numbers. There is also a need to automatically provide a safe mechanism to contact the entity, since it is uncertain if a given contact claiming to be from that entity is real or untrustworthy.

SUMMARY OF THE INVENTION

[0007] The present invention provides systems and methods for dynamically providing safe call back numbers to use to respond to an inbound communication as defined by accompanying claims 1 and 13, respectively. According to one embodiment, a system comprises a processor and a memory having executable instructions stored thereon that when executed by the processor cause the processor to parse a message or call history record and extract entity contact data from the parsed message or call history record. The entity contact data includes at least a phone number and alleged entity name. The processor is further configured to compare the extracted entity contact data with a reference data set that is retrieved from a database storing genuine and fraud data, where the genuine and fraud data includes entities and contact data corresponding to the entities, determine the entity contact data is not authentic based on the comparison of the entity contact data, and execute a remedy action based on the determination, the remedy action including a replacement of the phone number with an authentic phone number based on the determination.

[0008] The remedy action may be performed automatically, with user consent, in advance of an attempt to call the phone number, or in real-time as a user attempts to dial the phone number. The remedy action may further include a message that the phone number has been replaced. In another embodiment, the remedy action further includes a warning that the message or call history record includes fraudulent or other untrustworthy information. In another embodiment, the remedy action further includes blocking of a communicator of a message or call associated with the message or call history record from incoming and outgoing communications. In yet another embodiment, the remedy action further includes an insertion of a visual indicator or icon next to the phone number in the message or call history record that includes an alert that the phone number is suspicious. The visual indicator or icon may further include a link to call a correct number.

[0009] The processor can be further configured to determine that a communicator of a message or call

associated with the message or call history record is unwanted or suspicious based on the comparing of the entity contact data and determine the entity contact data is not authentic based on the determination that the communicator is unwanted or suspicious. The processor may also be configured to access an electronic message inbox. The message or call history record may comprise at least one of a voice message, a transcribed voice message, and a text message. The processor may be configured to parse the message or call history record by identifying information of interest. The processor may verify the entity contact data by performing at least one of caller carrier analysis, cellular/landline analysis, fingerprinting, and matching to a database of templates associated with fraudulent or suspicious messages. The system may comprise the processor further configured to replace the contact data in the message or call history record with verified contact data based on the determination that the contact data is not authentic. The processor may be further configured to identify caller identification data and confirm the alleged entity based on the caller identification data and a user contact list.

[0010] According to one embodiment, the system comprises a database including a reference data set, the reference data set including genuine and fraud data wherein the genuine and fraud data includes entities and contact information corresponding to the entities, a message scanning server communicatively coupled to a message server, the message scanning server configured to parse message records from the message server, analyze the message records for fraudulent or other untrustworthy phone numbers by comparing content of the message records to the reference data set, and determine untrustworthy phone numbers in the message records from the analysis, and a prescription rule server communicatively coupled to the message scanning server, the prescription rule server configured to generate remedy actions based on the determination of the untrustworthy phone numbers.

[0011] The remedy action may include at least one of preventing calls to the untrustworthy phone numbers, generating warnings of the untrustworthy phone numbers, and according to the invention, substituting the untrustworthy phone numbers in the message records with correct phone numbers. The genuine and fraud data may include numbers of legitimate calling entities. The genuine and fraud data may include known fraudulent numbers. The database may further comprise one or more of a fingerprinting database, a database of suspicious text and messaging patterns, a database of carriers and their scores, and a database of valid phone numbers. The message record may comprise at least one of voice messages, transcribed voice messages, and text messages. The message scanning server may be further configured to parse a call history record, extract contact data from the parsed call history record, compare the contact data with the reference data set, and determine the contact data is not authentic based on the comparison. The prescription rule server may be further configured to replace the contact data with verified contact data based on the determination that the contact data is not authentic.

[0012] According to one embodiment, the method comprises parsing message records from a message server, analyzing the message records for untrustworthy phone numbers by comparing content of the message records to a reference data set that is retrieved from a database, the reference data set including genuine and fraud data wherein the genuine and fraud data include entities and contact information corresponding to the entities, determining untrustworthy phone numbers in the message records from the analysis, and generating remedy actions based on the determination of the untrustworthy phone numbers.

[0013] The method may further comprise analyzing the message records by performing at least one of caller carrier analysis, cellular/landline analysis, fingerprinting, and matching to a database of templates associated with fraudulent or suspicious messages. The remedy action may include at least one of preventing calls to the untrustworthy phone numbers, generating warnings of the untrustworthy phone numbers, and according to the invention, substituting the untrustworthy phone numbers in the message records with correct phone numbers. The message records may comprise at least one of voice messages, transcribed voice messages, and text messages. The method may further comprise parsing a call history record, extracting entity contact data from the parsed call history record, comparing the extracted entity contact data with the reference data set, determining the entity contact data is not authentic based on the comparison, and replacing the contact data with verified contact data. The alleged entity may be confirmed based on caller identification data and a user contact list.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The invention is illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like references are intended to refer to like or corresponding parts.

Fig. 1 illustrates a computing system according to an embodiment of the present invention.

Fig. 2 illustrates a flowchart of a method for providing safe call back numbers according to an embodiment of the present invention.

Fig. 3 illustrates a computing system according to another embodiment of the present invention.

Fig. 4 illustrates a flowchart of a method for providing safe call back numbers according to an embodiment of the present invention.

Fig. 5 illustrates a flowchart of a method for replacing call back numbers according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] Subject matter will now be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, exemplary embodiments in which the invention may be practiced. Subject matter may, however, be embodied in a variety of different forms and, therefore, covered or claimed subject matter is intended to be construed as not being limited to any example embodiments set forth herein; example embodiments are provided merely to be illustrative. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention. Likewise, the phrase "in one embodiment" as used herein does not necessarily refer to the same embodiment and the phrase "in another embodiment" as used herein does not necessarily refer to a different embodiment. Among other things, for example, subject matter may be embodied as methods, devices, components, or systems. Accordingly, embodiments may, for example, take the form of hardware, software, firmware or any combination thereof (other than software per se). The following detailed description is, therefore, not intended to be taken in a limiting sense. The scope of protection is defined by the appended claims.

[0016] The present application discloses systems and methods for safely returning calls based on phone numbers in messages from unknown or unwanted callers or numbers. According to one embodiment, a system may comprise a server and/or client device executing code that scans a user's voice messages (either in audio or transcriptions), text messages, or caller identification ("caller ID") data history (e.g., of "missed calls"), and recognize phone numbers from the messages or caller ID data. The system may check the caller's phone number and identify the caller or determine if it's wanted or unwanted (using, for example, with white/black lists or with more advanced techniques as described in commonly owned U.S. Patent No. 10,051,121, entitled "SYSTEM AND METHOD FOR IDENTIFYING UNWANTED COMMUNICATIONS USING COMMUNICATION FINGERPRINTING"). The system may also provide an alternative or a guaranteed safe number that can be used to return a call, for times when a caller cannot be 100% trusted to be the number of a claimed entity.

[0017] If the caller's phone number is unknown or unwanted, the system may search and determine whether the phone number is either authentic or fraudulent or otherwise untrustworthy, e.g., by comparing it to a database of known numbers for who the caller claims to be. For example, if the caller claims to be from the user's bank, the system may compare the phone number against a database of phone numbers for the user's bank or all banks, as appropriate. The phone number can also be compared against a list of known scam or unwanted numbers. However, if the phone number left in the message fails to be authenticated, the system may prevent the call recipient from calling that phone number back but according to the invention the system substitutes the phone number in the message for an actual number for who that caller claims to be. For example, if the voice or text message from the caller says, "please contact Chase Bank regarding a potential fraud on your account," the system may substitute a fraudulent phone number provided in the message with an actual phone number corresponding to Chase Bank's fraud prevention line from a database. The system may inform or provide an indication to the user that the system is performing such a function or operation and give the user the option which phone number to call, or otherwise may just substitute the fraudulent phone number without notifying the user.

[0018] Fig. 1 presents a computing system according to an embodiment of the present invention. The system may comprise client device(s) 102 that are capable of establishing and receiving telephonic communications via communications network 108. The communications network 108 may include one or more public switch telephone networks, local area networks, wide area networks, the Internet, private VPN's (virtual private networks), or any other communications networks. In some embodiments, the client device(s) 102 are enabled with an application such as the one available from YouMail Inc., www.youmail.com, the assignee of the present patent application.

[0019] Client device(s) 102 may comprise computing devices capable of executing telephony-related applications and electronic messaging applications. Examples of computing devices include mobile smartphones, desktop computers, television set top boxes, laptops, personal digital assistants (PDA), tablet computers, e-book readers, smartwatches and smart wearable devices, or any computing device having a central processing unit and memory unit capable of connecting to a communications network. The computing device may also comprise a graphical user interface (GUI) or a browser application provided on a display (e.g., monitor screen, LCD or LED display, projector, etc.). A computing device may also include or execute an application to communicate content, such as, for example, textual content, multimedia content, or the like. A computing device may also include or execute an application to perform a variety of possible tasks, such as browsing, searching, playing various forms of content, including streamed audio. A computing device may include or execute a variety of operating systems, including a personal computer operating system, such as a Windows, Mac OS or Linux, or a mobile operating system, such as iOS, Android, or Windows Mobile, or the like. A computing device may include or may execute a variety of possible applications, such as a computing software application enabling communication with other devices, such as communicating one or more messages, such as via email, short message service (SMS), or multimedia message service (MMS).

[0020] The system further includes message server

104 which may perform voice mail operations such as recording (and/or transcribing) voice messages for subscribers of client device(s) 102. A user may enable fraud message scanning by providing a client application installed on client device(s) 102, message scanning server 106, or a combination of the two, with access to their electronic message inbox including, e.g., recorded or transcribed voice messages, and user call history (e.g., when people try to simply return a call often because of seeing the caller ID or just blindly calling). hosted on the message server 104 or stored locally on client device(s) 102. The recorded or transcribed voice messages and call history logs may be scanned by the client application or message scanning server 106 to detect fraud. According to one embodiment, the client application or message scanning server 106 may analyze communication feeds including voice messages, texts and emails for fraudulent phone numbers, email addresses, websites, or other contact information.

[0021] Servers, as described herein, may vary widely in configuration or capabilities but are comprised of at least a special-purpose digital computing device or system including at least one or more central processing units and memory. A server may also include one or more of mass storage devices, power supplies, wired or wireless network interfaces, input/output interfaces, and operating systems, such as Windows Server, Mac OS X, Unix, Linux, FreeBSD, or the like. In an example embodiment, a server may include or have access to memory for storing instructions or applications for the performance of various functions and a corresponding processor for executing stored instructions or applications. For example, the memory may store an instance of the server configured to operate in accordance with the disclosed embodiments.

[0022] The client application or message scanning server 106 may be connected to database(s) 110. Database(s) 110 may include a plurality of databases including a fingerprinting database, a database of suspicious text/messaging patterns, a database of carriers and their scores, and a database of valid phone numbers or communication addresses. The database(s) 110 may contain a reference data set that can be retrieved and used to analyze the content of the communication feeds by comparing information in the reference data set against, for example, phone numbers, email addresses, websites, or contact information in the content of the communication feeds. The reference data set may include genuine and fraud data which include entities (legitimate and fraudulent) and their corresponding contact information. Genuine data may comprise lists of correct or verified phone numbers or contact information of, for example, safe entities (e.g., banks, car or credit card companies, the IRS, other call centers) who may supply their phone numbers to database(s) 110. Fraud data may comprise phone numbers or contact information of unsafe entities. Call directory servers, call screening systems, and other spam detection services may provide fraud information including lists of known fraudulent phone numbers to database(s) 110 as they are identified. For example, the client application or message scanning server 106 may determine a phone number or caller ID data in a message (or call history) is either authentic or fraudulent by comparing it to database(s) 110 of known numbers for who a caller claims to be. The phone number or caller ID data can also be compared against a list of known scam or unwanted numbers in database(s) 110.

[0023] The client application or message scanning server 106 may also be connected to a prescription rule server 112. The prescription rule server 112 may generate an executable remedy action which may dictate what actions are to be taken based on the analysis of the messages. If a phone number or other identification information left in an analyzed message or call history log is determined to be fraudulent or fails to be authenticated, prescription rule server 112 may direct the application or message scanning server 106 to prevent the recipient of the call or message from communicating with the fraudulent phone number (or block access to a link or address), generate a warning of the fraudulent phone number or identification information, or substitute the fraudulent phone number or identification information in the message or call history log with a verified number or contact information for who that caller claims to be. In certain embodiments, prescription rule server 112 may be deployed within the client application.

[0024] Message scanning and remediation can be performed either when messages or calls are received, or when a user selects a number from the message/call history to call. In one embodiment, a remedy action may include the client application inserting a visual indicator or icon next to the number in the message, such as a red star, or an exclamation point, to alert the user that the number is suspicious and should not be called. The icon may include a link which the user can select to call the correct/genuine number instead. Alternatively, the system may perform a scan and remedy action upon the client application detecting an instance where a user is trying to make a call or communication using a link in a message. According to another embodiment, the user may be prompted to perform a check or scan of the user's messages and/or call history logs. The user may be prompted with a message, such as "you're trying to return a call based on a number left in a message which might be suspicious, would you like us to check it first?"

[0025] Fig. 2 presents a flowchart of a method for providing safe call back numbers according to an embodiment of the present invention. Users may authenticate the content of their messages by allowing a message scanning system to access their message inboxes that are hosted on a message server. Alternatively, the system may also authenticate numbers in a user's call history on a user's client device, such as for "missed calls." The authentication may be initiated automatically (e.g., in the background) or in real-time (e.g., as a user accesses a message or about to dial a number in the

message). Authenticating the content may include parsing a message (or call history) record, step 202. The message or call history record may include files, data, or other forms of information that may be retrieved from an electronic or virtual inbox on a message server, or on the user's client device, and may comprise a voice message, a transcribed voice message, a text message, or any other message format. Parsing a message or call history record may include identifying information of interest, such as sender/communicator name, metadata, a return phone number or email address, caller ID information, etc.

[0026] Entity contact data is extracted from the parsed message (or call history) record, step 204. The entity contact data may include a phone number, email address, or identifier and an alleged identity of the originator of the message, or anyone of the information of interest. The entity contact data is compared with a reference data set, step 206. Comparing the entity contact data may include analysis by cross referencing the entity contact data with genuine and fraud data which is related to entities (legitimate and fraudulent) and their contact information. For example, the system may compare a phone number and an alleged entity in the message record to a correct phone number associated with the alleged entity. The system may also use information that is associated with a call or message to identify and/or confirm an identity of an entity, such as incoming caller ID as well as the user's contact lists (e.g., information stored in their address book).

[0027] The analysis of the entity contact data may account for different information from the reference data set to decide whether a communicator is unwanted or suspicious. For example, comparing the entity contact data may include one or more of the following analysis:

(i) Caller carrier analysis - A carrier of the communicator's phone number may be determined and used to retrieve a score of the carrier. The carrier score may be used to determine whether a return phone number is trustworthy. A message from a communicator with a phone number having a low or untrustworthy carrier score may be flagged as suspicious.

(ii) Cellular/landline analysis - The system may determine whether a communicator's phone number is a cellular or landline number. Since a call from a bank, automobile company, credit card company, and other help or call centers for major companies are primarily landlines and not cellular phone numbers. As such, communicators using cellular phone numbers may be treated suspiciously.

(iii) Fingerprinting - A "fingerprint" of a message or text may be created and compared with a database of fingerprints of known recordings of calls or messages (voice and/or text) from unwanted or wanted communicators by using speech processing, natural language processing, and machine learning algorithms with the information accumulated from the variety of sources. A fingerprint may comprise a unique identification of a sequence of characters designed to capture the content of, for example, a commonly appearing or known voice message. The unique identification may include a representation of text content data including keywords or tags, and an emphasis of importance of each keyword or tag that may be indicated with a variety of indicators, such as, ranking, arrangement, classification, word count, font size and color. Based on a comparison of the fingerprint of the message or text with the database of fingerprints, the system may determine whether the communicator is unwanted and suspicious and treat the entity contact data of the message record accordingly. Fingerprinting is described in further detail in commonly owned U.S. Patent No. 10,051,121, issued on August 14, 2018, entitled "SYSTEM AND METHOD FOR IDENTIFYING UNWANTED COMMUNICATIONS USING COMMUNICATION FINGERPRINTING,".

(iv) Match the message against a database of templates of fraudulent or suspicious messages - Textual messages or voice messages, for example, may be collected from a plurality of users into a database and analyzed for fraudulent and suspicious activity. Fraudulent messages may be used to create templates of fraudulent or suspicious messages for comparison with a given message. The templates may also include known patterns or attributes of fraudulent messages. The known patterns or attributes of fraudulent messages may include certain keywords or phrases commonly associated with scammers, telemarketer, etc.

[0028] A determination is made whether the entity contact data is authentic based on the verification, step 208. The determination may perform one or more of the aforementioned analysis and weigh results of the analysis according to certain thresholds. For example, one or more scores may be calculated for the entity contact data based on certain authenticity criteria. If given scores of one or more criteria exceed satisfactory thresholds, the entity contact data may be deemed authentic. According to one embodiment, a threshold for what constitutes a suspicious message or call may be lower given that the system is not necessarily blocking the message or communicator. Additionally, if the communicator is determined to be unwanted or suspicious, the entity contact data of the message may be determined as suspicious or fraudulent (e.g., not authentic). Otherwise, the message record (or a number in the user's call history) may be deemed authentic.

[0029] If the entity contact data is determined to be authentic, communication corresponding to the entity

contact data may be allowed, step 210. That is, the user may be allowed to access/dial a link, number, or address in the message (or call history log). However, if the entity contact data is determined to be not authentic, a remedy action may be executed, step 212. Various remedy actions may be generated based on authenticity scoring. The remedy action may include at least one of generating a warning that the message contains fraudulent information, substituting content in the message record (or user call history) with verified information (e.g., with a safe/-correct number or contact information), or blocking the communicator/sender of the message from incoming and outgoing communications. Accordingly, scaling of actions may correlate with the authenticity scoring.

[0030] Fig. 3 presents a computing system according to another embodiment of the present invention. Computing system 300 may comprise a retrieval unit 302 that can access a user's messages and call histories by communicating with a user's client device via application interface 304. The retrieval unit 302 may either retrieve messages and call histories directly from the user's client device or given permission/credentials to download the user's messages from a message server. Upon retrieval of the user's messages or call histories, parser 306 may parse the messages or call history entries to identify information of interest, such as sender/communicator name, metadata, a return phone number or email address, caller ID information, etc.

[0031] Content analyzer 308 may extract the information that is parsed by the parser 306. The extracted information may be analyzed by content analyzer 308 in accordance with a reference data set that can be retrieved from one or more databases through database interface 310. The extracted information may be cross referenced with the reference data set which may include correct information of safe entities and/or fraudulent information of unsafe entities. The content analyzer 308 may further determine whether the extracted information is either authentic or fraudulent based on a verification with the reference data set. For example, the content analyzer 308 may determine fraudulent phone numbers in the extracted information.

[0032] Content analyzer 308 may send results of analysis to prescription rule module 312. Prescription rule module 312 is operable to generate or provide remedy actions based on the determination of the fraudulent phone numbers. Remedy actions may comprise executable instructions that may be transmitted to the user's client device through application interface 304. The remedy actions may instruct the user's client device to perform certain operations if the message or call history is determined to include fraudulent information (e.g., fake caller ID). Exemplary remedy actions may include generating a warning that the message or call history contains fraudulent information, substituting content in the message with verified information (e.g., with a safe/correct number or contact information), or blocking the communicator/sender of the message from incoming and outgoing communications.

[0033] Fig. 4 presents a flowchart of a method for providing safe call back numbers according to one embodiment. For any inbound call or message, a computing system may determine who a claimed caller actually is, and whether that caller is entirely trustable. A message or caller ID from a missed call data may be scanned by a computing system for an untrusted call back number. The message may comprise voice or text messages. Messages may be processed using natural language analyzers and phrase detection algorithms. A phone number in a message is identified, step 402. The phone number may be an untrusted phone number that a caller may want a recipient of the message to call or dial.

[0034] An entity that is alleged in the message is determined, step 404. For example, a caller leaving the message may claim to be associated with an entity, such as a bank or credit card company. A correct phone number for the entity is determined, step 406. The correct phone number may be determined by retrieving a phone number associated with the entity from a trusted data source.

[0035] The system determines whether the phone number in the message is the correct phone number, step 408. The phone number may be compared with the retrieved phone number. The system may also compare the phone number with a database including genuine and fraud data. Additionally, techniques, such as Signature-based Handling of Asserted Information Using toKENs ("SHAKEN") and Secure Telephone Identity Revisited ("STIR") may be used to authenticate the phone number. SHAKEN/STIR verification may comprise callers having their caller ID "signed" as legitimate by originating carriers and validated by a service provider at the destination to verify that an incoming call is really coming from a number listed on a caller ID display. If the phone number in the message is the same as the correct phone number, the message is determined to be safe, step 410. Otherwise, the phone number in the message is replaced with the correct phone number, step 412.

[0036] Fig. 5 presents a flowchart of a method for replacing call back numbers according to an embodiment of the present invention. A computing system initializes configurations for scanning a user's messages (or call history), step 502. The system determines whether automatic replacement has been selected, step 504. Configuring for automatic replacement may allow the computing system to directly proceed to scan a message, step 512. If not, the system may determine if the user has consented to scan a message, step 506. Consenting to the scan may be an on-demand request.

[0037] If the user has not consented to the scan, the system waits for user action, step 508. The system check determines if a user's actions requires a real-time response, such as attempting to dial a phone number contained within the message (or call history). If a real-time response is triggered, the system proceeds to scan the message at step 512. On the other hand, a user action

that does not require a real-time response, the system may loop back to step 506 to wait for the user's consent. Receiving the user consent allows the computing system to scan the message at step 512.

[0038] The computing system can determine whether a phone number in the scanned message (or call history) is correct for an entity asserted in the message, step 514, by consulting a reference data set or a database storing genuine and fraud data. A correct phone number may be retrieved for the asserted entity and compared with the phone number in the message. A message is determined to be safe if the phone number is correct, step 516.

[0039] If the phone number is not correct, the user may be optionally notified of a replacement of the phone number in the message (or call history), step 518. The option may be configured with a setting by the user or predefined by the system. If no notification is needed, the system replaces the phone number in the message (or the user's call history log) with the correct phone number, step 520. A message that indicates the replacement is generated if the user is to be notified, step 522, prior to replacing the phone number.

[0040] Figures 1 through 5 are conceptual illustrations allowing for an explanation of the present invention. Notably, the figures and examples above are not meant to limit the scope of the present invention to a single embodiment, as other embodiments are possible by way of interchange of some or all of the described or illustrated elements. Moreover, where certain elements of the present invention can be partially or fully implemented using known components, only those portions of such known components that are necessary for an understanding of the present invention are described, and detailed descriptions of other portions of such known components are omitted so as not to obscure the invention. In the present specification, an embodiment showing a singular component should not necessarily be limited to other embodiments including a plurality of the same component, and vice-versa, unless explicitly stated otherwise herein. Moreover, applicants do not intend for any term in the specification or claims to be ascribed an uncommon or special meaning unless explicitly set forth as such. Further, the present invention encompasses present and future known equivalents to the known components referred to herein by way of illustration.

[0041] It should be understood that various aspects of the embodiments of the present invention could be implemented in hardware, firmware, software, or combinations thereof. In such embodiments, the various components and/or steps would be implemented in hardware, firmware, and/or software to perform the functions of the present invention. That is, the same piece of hardware, firmware, or module of software could perform one or more of the illustrated blocks (*e.g.,* components or steps). In software implementations, computer software (*e.g.,* programs or other instructions) and/or data is stored on a machine-readable medium as part of a computer program product and is loaded into a computer system or other device or machine via a removable storage drive, hard drive, or communications interface. Computer programs (also called computer control logic or computer-readable program code) are stored in a main and/or secondary memory, and executed by one or more processors (controllers, or the like) to cause the one or more processors to perform the functions of the invention as described herein. In this document, the terms "machine readable medium," "computer-readable medium," "computer program medium," and "computer usable medium" are used to generally refer to media such as a random access memory (RAM); a read only memory (ROM); a removable storage unit (*e.g.,* a magnetic or optical disc, flash memory device, or the like); a hard disk; or the like.

[0042] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the relevant art(s) readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Such adaptations and modifications are therefore intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance presented herein, in combination with the knowledge of one skilled in the relevant art(s).

Claims

1. A system (104, 106, 112, 300) for providing safe call back numbers, the system comprising:

a processor; and

a memory having executable instructions stored thereon that when executed by the processor cause the processor to:

parse a message record (202), the message record comprising a text or voice message left or sent by a communicator;

extract entity contact data from content of the parsed message record (204), the entity contact data including at least a phone number and data representing an identity of an alleged legitimate entity including at least a name associated with the alleged legitimate entity;

compare the extracted entity contact data with a reference data set (206) that is retrieved from a database (110) storing genuine and fraud data, the reference data set including legitimate entities and contact

data corresponding to the legitimate entities;
determine the entity contact data is not authentic (208) based on the extracted entity contact data not matching the contact data corresponding to the legitimate entities in the comparison; and
execute a remedy action (212) based on the determination, the remedy action including a replacement of the phone number in the message record with a safe call back number, from the database (110), of the legitimate entity the communicator claims to be according to the extracted entity contact data.

2. The system of claim 1 wherein the remedy action further includes a message that the phone number has been replaced (522).

3. The system of claim 1 or claim 2 wherein the remedy action is performed in advance of an attempt to call the phone number.

4. The system of claim 1 or claim 2 wherein the remedy action is performed in real-time as a user attempts to dial the phone number.

5. The system of any one of claims 1 to 4 wherein the remedy action further includes a warning that the message record includes fraudulent information.

6. The system of any one of claims 1 to 5 wherein the remedy action further includes blocking of the communicator from incoming and outgoing communications.

7. The system of any one of claims 1 to 6 wherein the remedy action further includes an insertion of a visual indicator or icon next to the phone number in the message record that includes an alert that the phone number is suspicious.

8. The system of any one of claims 1 to 7 wherein the processor is further configured to:

determine that the communicator is unwanted or suspicious based on the comparing; and
determine the entity contact data is not authentic based on the determination that the communicator is unwanted or suspicious.

9. The system of any one of claims 1 to 8 wherein the message record comprises a transcribed voice message.

10. The system of any one of claims 1 to 9 wherein the processor is further configured to perform at least one of caller carrier analysis, cellular/landline analysis, fingerprinting, and matching to a database of templates associated with fraudulent or suspicious messages.

11. The system of any one of claims 1 to 10 wherein the processor is further configured to replace the entity contact data in the message record with verified contact data based on the determination that the contact data is not authentic.

12. The system of any one of claims 1 to 11 wherein the processor is further configured to:

identify caller identification data; and
confirm the identity based on the caller identification data and a user contact list.

13. A method, in a data processing system (104, 106, 112, 300) comprising a processor and a memory, for providing safe call back numbers, the method comprising:

parsing (202, 306), by the data processing system, message records from a message server, the message records comprising text or voice messages left or sent by communicators;
analyzing (204, 308), by the data processing system, the message records for untrustworthy phone numbers by comparing contact information from content of the text or voice messages of the message records to contact information corresponding to legitimate entities in a reference data set that is retrieved from a database (110), the reference data set
including genuine and fraud data wherein the genuine and fraud data includes entities that are legitimate and contact information corresponding to the entities, and the contact information from the content of the text or voice messages including at least a phone number and data representing an identity of an alleged legitimate entity including at least a name associated with the alleged legitimate entity;
determining (206), by the data processing system, untrustworthy phone numbers in the message records based on the contact information from the content of the text or voice messages not matching the contact information corresponding to the legitimate entities in the reference data set from the analysis; and
generating (212), by the data processing system, remedy actions based on the determination of the untrustworthy phone numbers, wherein the remedy actions include a replacement of the untrustworthy phone numbers in the message records with safe call back numbers, from the database (110), of the legitimate entities the

communicators claim to be according to the extracted entity contact data.

14. The method of claim 13 further comprising analyzing the message records by performing at least one of caller carrier analysis, cellular/landline analysis, fingerprinting, and matching to a database of templates associated with untrustworthy or suspicious messages.

15. The method of claim 13 or claim 14 wherein the remedy action includes at least one of preventing calls to the untrustworthy phone numbers and generating warnings of the untrustworthy phone numbers.

Patentansprüche

1. System (104, 106, 112, 300) zum Bereitstellen sicherer Rückrufnummern, wobei das System umfasst:

einen Prozessor; und
einen Speicher, welcher ausführbare Anweisungen darauf gespeichert hat, welche, wenn von dem Prozessor ausgeführt, den Prozessor dazu veranlassen:

einen Nachrichtendatensatz (202) zu parsen, wobei der Nachrichtendatensatz eine von einem Zeichengeber hinterlassene oder gesendete Text-oder Sprachnachricht umfasst;
Entitätskontaktdaten aus dem Inhalt des geparsten Nachrichtendatensatzes (204) zu extrahieren, wobei die Entitätskontaktdaten zumindest eine Telefonnummer und Daten beinhalten, welche eine Identität einer angeblich legitimen Entität darstellen, welche zumindest einen mit der angeblich legitimen Entität verknüpften Namen beinhaltet;
die extrahierten Entitätskontaktdaten mit einem Referenzdatensatz (206) zu vergleichen, welcher aus einer Datenbank (110) abgerufen wird, in welcher echte und Betrugsdaten gespeichert sind, wobei der Referenzdatensatz legitime Entitäten und den legitimen Entitäten entsprechende Kontaktdaten beinhaltet;
zu bestimmen, dass die Entitätskontaktdaten nicht authentisch sind (208), basierend darauf, dass die extrahierten Entitätskontaktdaten nicht mit den Kontaktdaten übereinstimmen, welche den legitimen Entitäten in dem Vergleich entsprechen; und
basierend auf der Bestimmung eine Abhilfemaßnahme (212) auszuführen, wobei die Abhilfemaßnahme einen Austausch der Telefonnummer in dem Nachrichtendatensatz durch eine sichere Rückrufnummer aus der Datenbank (110) der legitimen Entität beinhaltet, welche der Zeichengeber gemäß den extrahierten Entitätskontaktdaten zu sein behauptet.

2. System nach Anspruch 1, wobei die Abhilfemaßnahme weiter eine Nachricht beinhaltet, dass die Telefonnummer ausgetauscht wurde (522).

3. System nach Anspruch 1 oder Anspruch 2, wobei die Abhilfemaßnahme vor einem Versuch, die Telefonnummer anzurufen, durchgeführt wird.

4. System nach Anspruch 1 oder Anspruch 2, wobei die Abhilfemaßnahme in Echtzeit durchgeführt wird, während ein Benutzer versucht, die Telefonnummer zu wählen.

5. System nach einem der Ansprüche 1 bis 4, wobei die Abhilfemaßnahme weiter eine Warnung beinhaltet, dass der Nachrichtendatensatz betrügerische Informationen beinhaltet.

6. System nach einem der Ansprüche 1 bis 5, wobei die Abhilfemaßnahme weiter Blockieren des Zeichengebers für eingehende und ausgehende Kommunikationen beinhaltet.

7. System nach einem der Ansprüche 1 bis 6, wobei die Abhilfemaßnahme weiter ein Einfügen eines visuellen Indikators oder Symbols neben der Telefonnummer in dem Nachrichtendatensatz beinhaltet, welcher eine Warnung beinhaltet, dass die Telefonnummer verdächtig ist.

8. System nach einem der Ansprüche 1 bis 7, wobei der Prozessor weiter dazu konfiguriert ist:

basierend auf dem Vergleichen zu bestimmen, dass der Zeichengeber unerwünscht oder verdächtig ist;
und
basierend auf der Bestimmung, dass der Zeichengeber unerwünscht oder verdächtig ist, zu bestimmen, dass die Entitätskontaktdaten nicht authentisch sind.

9. System nach einem der Ansprüche 1 bis 8, wobei der Nachrichtendatensatz eine transkribierte Sprachnachricht umfasst.

10. System nach einem der Ansprüche 1 bis 9, wobei der Prozessor weiter dazu konfiguriert ist, zumindest eines von einer Anruferträgeranalyse, Mobil-

funk-/Festnetzanalyse, Fingerabdruck und Abgleich mit einer Datenbank von Vorlagen, welche mit betrügerischen oder verdächtigen Nachrichten verknüpft sind, durchzuführen.

11. System nach einem der Ansprüche 1 bis 10, wobei der Prozessor weiter dazu konfiguriert ist, basierend auf der Bestimmung, dass die Kontaktdaten nicht authentisch sind, die Entitätskontaktdaten in dem Nachrichtendatensatz durch verifizierte Kontaktdaten zu ersetzen.

12. System nach einem der Ansprüche 1 bis 11, wobei der Prozessor weiter dazu konfiguriert ist:

Anruferidentifikationsdaten zu identifizieren; und
die Identität basierend auf den Anruferidentifikationsdaten und einer Benutzerkontaktliste zu bestätigen.

13. Verfahren in einem Datenverarbeitungssystem (104, 106, 112, 300), welches einen Prozessor und einen Speicher umfasst, zum Bereitstellen sicherer Rückrufnummern, wobei das Verfahren umfasst:

Parsen (202, 306) von Nachrichtendatensätzen von einem Nachrichtenserver durch das Datenverarbeitungssystem, wobei die Nachrichtendatensätze von Zeichengebern hinterlassene oder gesendete Text- oder Sprachnachrichten umfassen;
Analysieren (204, 308) der Nachrichtendatensätze auf nicht vertrauenswürdige Telefonnummern durch das Datenverarbeitungssystem durch Vergleichen von Kontaktinformationen aus dem Inhalt der Text- oder Sprachnachrichten der Nachrichtendatensätze mit Kontaktinformationen, welche legitimen Entitäten in einem Referenzdatensatz entsprechen, welcher aus einer Datenbank (110) abgerufen wird, wobei der Referenzdatensatz
echte und Betrugsdaten beinhaltet, wobei die echten und Betrugsdaten legitime Entitäten und den Entitäten entsprechende Kontaktinformationen beinhalten und die Kontaktinformationen aus dem Inhalt der Text- oder Sprachnachrichten zumindest eine Telefonnummer und Daten beinhalten, welche eine Identität einer angeblich legitimen Entität darstellen, welche zumindest einen mit der angeblich legitimen Entität verknüpften Namen beinhaltet;
Bestimmen (206), durch das Datenverarbeitungssystem, nicht vertrauenswürdiger Telefonnummern in den Nachrichtendatensätzen basierend auf den Kontaktinformationen aus dem Inhalt der Text- oder Sprachnachrichten, welche nicht mit den Kontaktinformationen übereinstimmen, welche den legitimen Entitäten in dem Referenzdatensatz aus der Analyse entsprechen; und
Generieren (212) von Abhilfemaßnahmen basierend auf der Bestimmung der nicht vertrauenswürdigen Telefonnummern durch das Datenverarbeitungssystem, wobei die Abhilfemaßnahmen einen Austausch der nicht vertrauenswürdigen Telefonnummern in den Nachrichtendatensätzen durch sichere Rückrufnummern aus der Datenbank (110) der legitimen Entitäten beinhalten, welche die Zeichengeber gemäß den extrahierten Entitätskontaktdaten zu sein behaupten.

14. Verfahren nach Anspruch 13, welches weiter Analysieren der Nachrichtendatensätze durch Durchführen von zumindest einem von Anruferträgeranalyse, Mobilfunk-/Festnetzanalyse, Fingerabdruck und Abgleich mit einer Datenbank von Vorlagen umfasst, welche mit nicht vertrauenswürdigen oder verdächtigen Nachrichten verknüpft sind.

15. Verfahren nach Anspruch 13 oder Anspruch 14, wobei die Abhilfemaßnahme zumindest eines von Verhindern von Anrufen an die nicht vertrauenswürdigen Telefonnummern und Generieren von Warnungen vor den nicht vertrauenswürdigen Telefonnummern beinhaltet.

Revendications

1. Système (104, 106, 112, 300) pour fournir des numéros de rappel sûrs, le système comprenant :

un processeur ; et
une mémoire présentant des instructions exécutables stockées sur celle-ci qui, lorsqu'elles sont exécutées par le processeur, amènent le processeur à :

analyser syntaxiquement un enregistrement de message (202), l'enregistrement de message comprenant un message textuel ou vocal laissé ou envoyé par un communicateur ;
extraire des données de contact d'entité du contenu de l'enregistrement de message analysé syntaxiquement (204), les données de contact d'entité incluant au moins un numéro de téléphone et des données représentant une identité d'une entité prétendument légitime incluant au moins un nom associé à l'entité prétendument légitime ;
comparer les données de contact d'entité extraites à un jeu de données de référence

(206) qui est récupéré d'une base de données (110) stockant des données authentiques et frauduleuses, le jeu de données de référence incluant des entités légitimes et des données de contact correspondant aux entités légitimes ;
déterminer que les données de contact d'entité ne sont pas authentiques (208) sur la base du fait que les données de contact d'entité extraites ne correspondent pas aux données de contact correspondant aux entités légitimes dans la comparaison ; et
exécuter une action corrective (212) sur la base de la détermination, l'action corrective incluant un remplacement du numéro de téléphone dans l'enregistrement de message par un numéro de rappel sûr, à partir de la base de données (110), de l'entité légitime que le communicateur prétend être selon les données de contact d'entité extraites.

2. Système selon la revendication 1, dans lequel l'action corrective inclut en outre un message indiquant que le numéro de téléphone a été remplacé (522).

3. Système selon la revendication 1 ou la revendication 2, dans lequel l'action corrective est effectuée avant une tentative d'appel du numéro de téléphone.

4. Système selon la revendication 1 ou la revendication 2, dans lequel l'action corrective est effectuée en temps réel pendant qu'un utilisateur tente de composer le numéro de téléphone.

5. Système selon l'une quelconque des revendications 1 à 4, dans lequel l'action corrective inclut en outre un avertissement indiquant que l'enregistrement de message inclut des informations frauduleuses.

6. Système selon l'une quelconque des revendications 1 à 5, dans lequel l'action corrective inclut en outre l'interdiction au communicateur d'effectuer des communications entrantes et sortantes.

7. Système selon l'une quelconque des revendications 1 à 6, dans lequel l'action corrective inclut en outre une insertion d'un indicateur visuel ou d'une icône à côté du numéro de téléphone dans l'enregistrement de message qui inclut une alerte indiquant que le numéro de téléphone est suspect.

8. Système selon l'une quelconque des revendications 1 à 7, dans lequel le processeur est en outre configuré pour :

déterminer que le communicateur est indésirable ou suspect sur la base de la comparaison ; et
déterminer que les données de contact d'entité ne sont pas authentiques sur la base de la détermination que le communicateur est indésirable ou suspect.

9. Système selon l'une quelconque des revendications 1 à 8, dans lequel l'enregistrement de message comprend un message vocal transcrit.

10. Système selon l'une quelconque des revendications 1 à 9, dans lequel le processeur est en outre configuré pour effectuer au moins une d'une analyse d'opérateur appelant, d'une analyse de téléphonie mobile/fixe, d'empreintes digitales et d'une correspondance avec une base de données de modèles associés à des messages frauduleux ou suspects.

11. Système selon l'une quelconque des revendications 1 à 10, dans lequel le processeur est en outre configuré pour remplacer les données de contact d'entité dans l'enregistrement de message par des données de contact vérifiées sur la base de la détermination que les données de contact ne sont pas authentiques.

12. Système selon l'une quelconque des revendications 1 à 11, dans lequel le processeur est en outre configuré pour :

identifier des données d'identification d'appelant ; et
confirmer l'identité sur la base des données d'identification d'appelant et d'une liste de contacts d'utilisateur.

13. Procédé dans un système de traitement de données (104, 106, 112, 300) comprenant un processeur et une mémoire pour fournir des numéros de rappel sûrs, le procédé comprenant :

l'analyse syntaxique (202, 306), par le système de traitement de données, d'enregistrements de messages provenant d'un serveur de messages, les enregistrements de messages comprenant des messages textuels ou vocaux laissés ou envoyés par des communicateurs ;
l'analyse (204, 308), par le système de traitement de données, des enregistrements de messages pour des numéros de téléphone non fiables en comparant des informations de contact provenant du contenu des messages textuels ou vocaux des enregistrements de messages à des informations de contact correspondant à des entités légitimes dans un jeu de données de référence qui est récupéré à partir d'une base de données (110), le jeu de données de réfé-

rence incluant des données authentiques et frauduleuses, dans lequel les données authentiques et frauduleuses incluent des entités qui sont légitimes et des informations de contact correspondant aux entités, et les informations de contact provenant du contenu des messages textuels ou vocaux incluant au moins un numéro de téléphone et des données représentant une identité d'une entité prétendument légitime incluant au moins un nom associé à l'entité prétendument légitime ;

la détermination (206), par le système de traitement de données, de numéros de téléphone non fiables dans les enregistrements de messages sur la base des informations de contact provenant du contenu des messages textuels ou vocaux ne correspondant pas aux informations de contact correspondant aux entités légitimes dans le jeu de données de référence provenant de l'analyse ; et

la génération (212), par le système de traitement de données, d'actions correctives sur la base de la détermination des numéros de téléphone non fiables, dans lequel les actions correctives incluent un remplacement des numéros de téléphone non fiables dans les enregistrements de messages par des numéros de rappel sûrs, à partir de la base de données (110), des entités légitimes que les communicateurs prétendent être selon les données de contact d'entité extraites.

14. Procédé selon la revendication 13 comprenant en outre l'analyse des enregistrements de messages en effectuant au moins une d'une analyse d'opérateur appelant, d'une analyse de téléphonie mobile/-fixe, d'empreintes digitales et d'une correspondance avec une base de données de modèles associés à des messages non fiables ou suspects.

15. Procédé selon la revendication 13 ou la revendication 14, dans lequel l'action corrective inclut au moins une de l'interdiction d'appels vers les numéros de téléphone non fiables et de la génération d'avertissements concernant les numéros de téléphone non fiables.

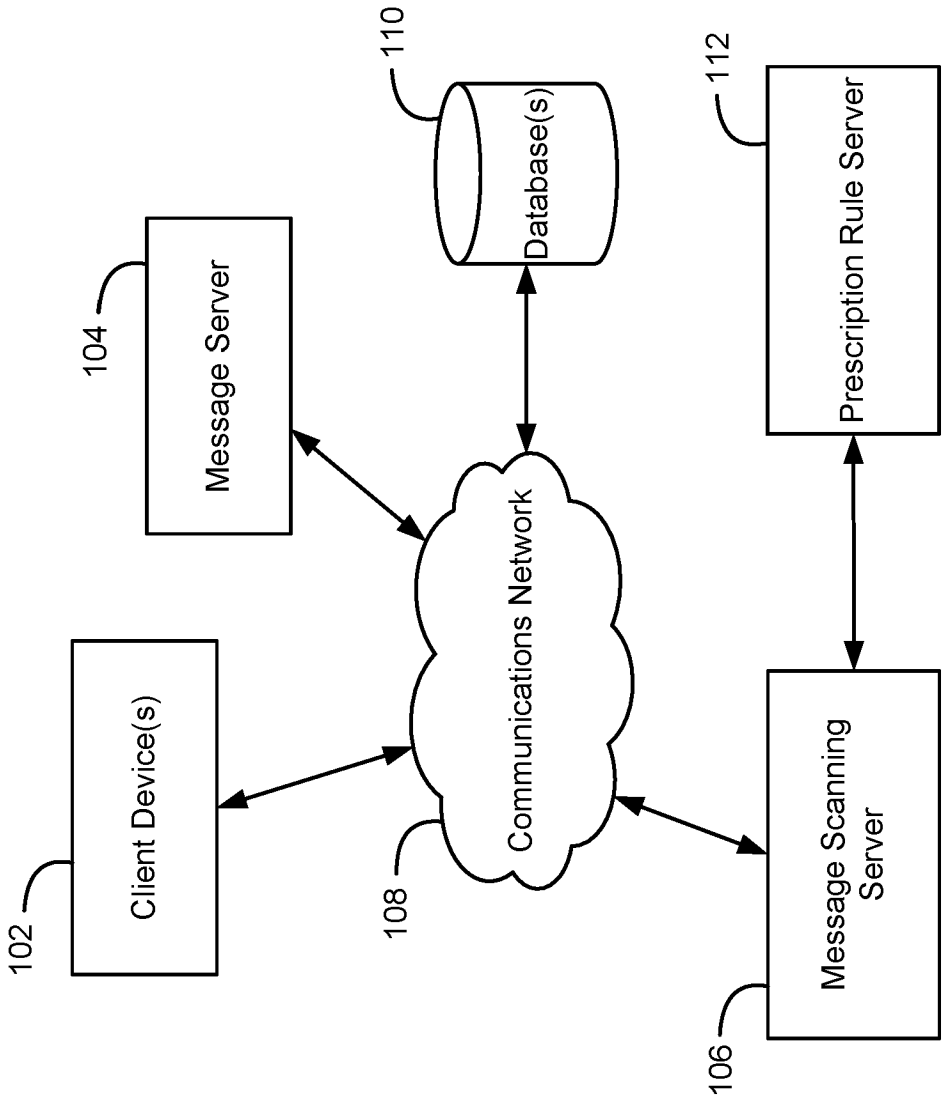
Client Device(s)
102
Message Server
104
Communications Network
108
Database(s)
110
Message Scanning Server
106
Prescription Rule Server
112

Fig. 1

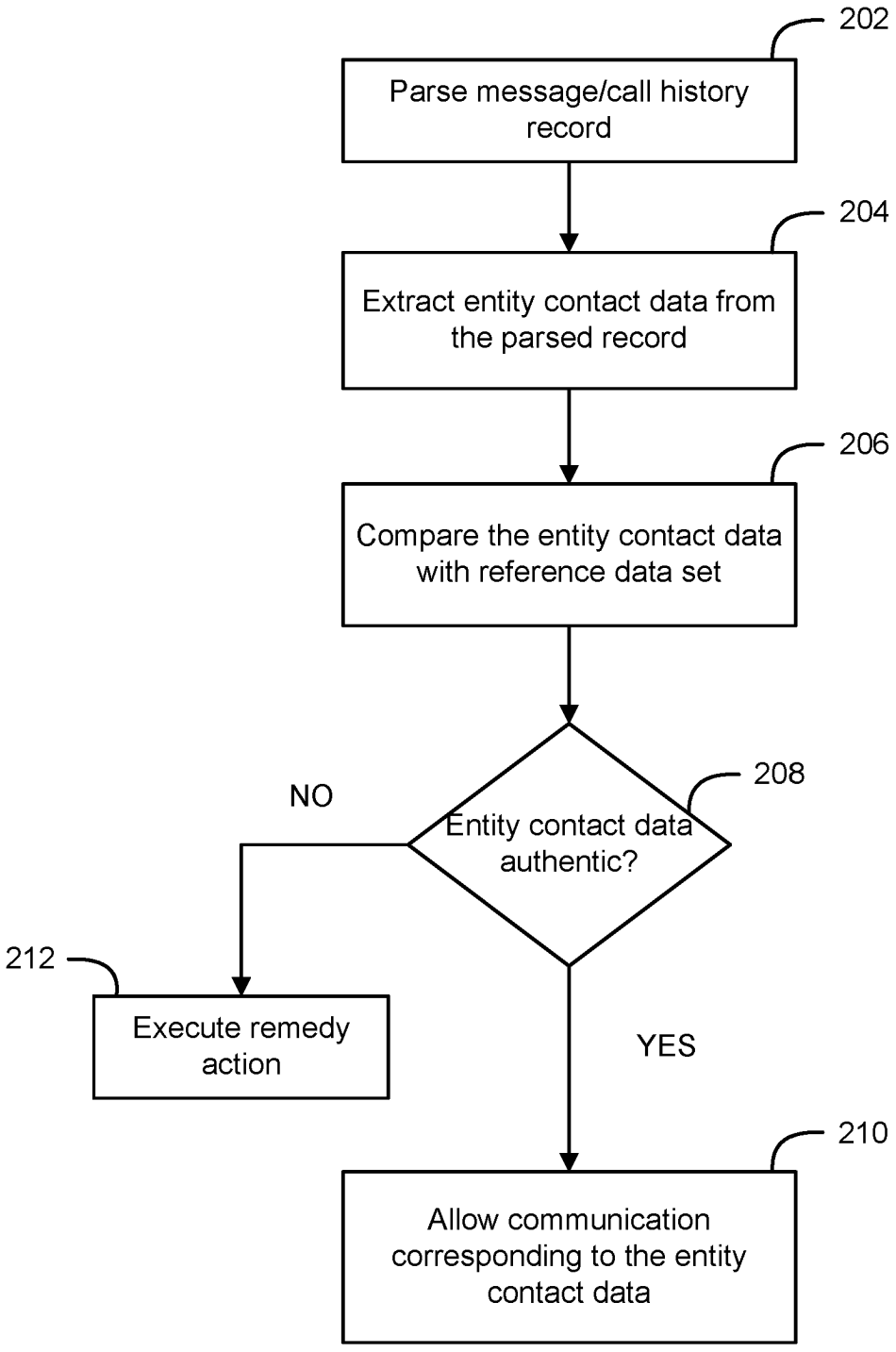
202
Parse message/call history record
204
Extract entity contact data from the parsed record
206
Compare the entity contact data with reference data set
208
Entity contact data authentic?
NO
YES
212
Execute remedy action
210
Allow communication corresponding to the entity contact data

Fig. 2

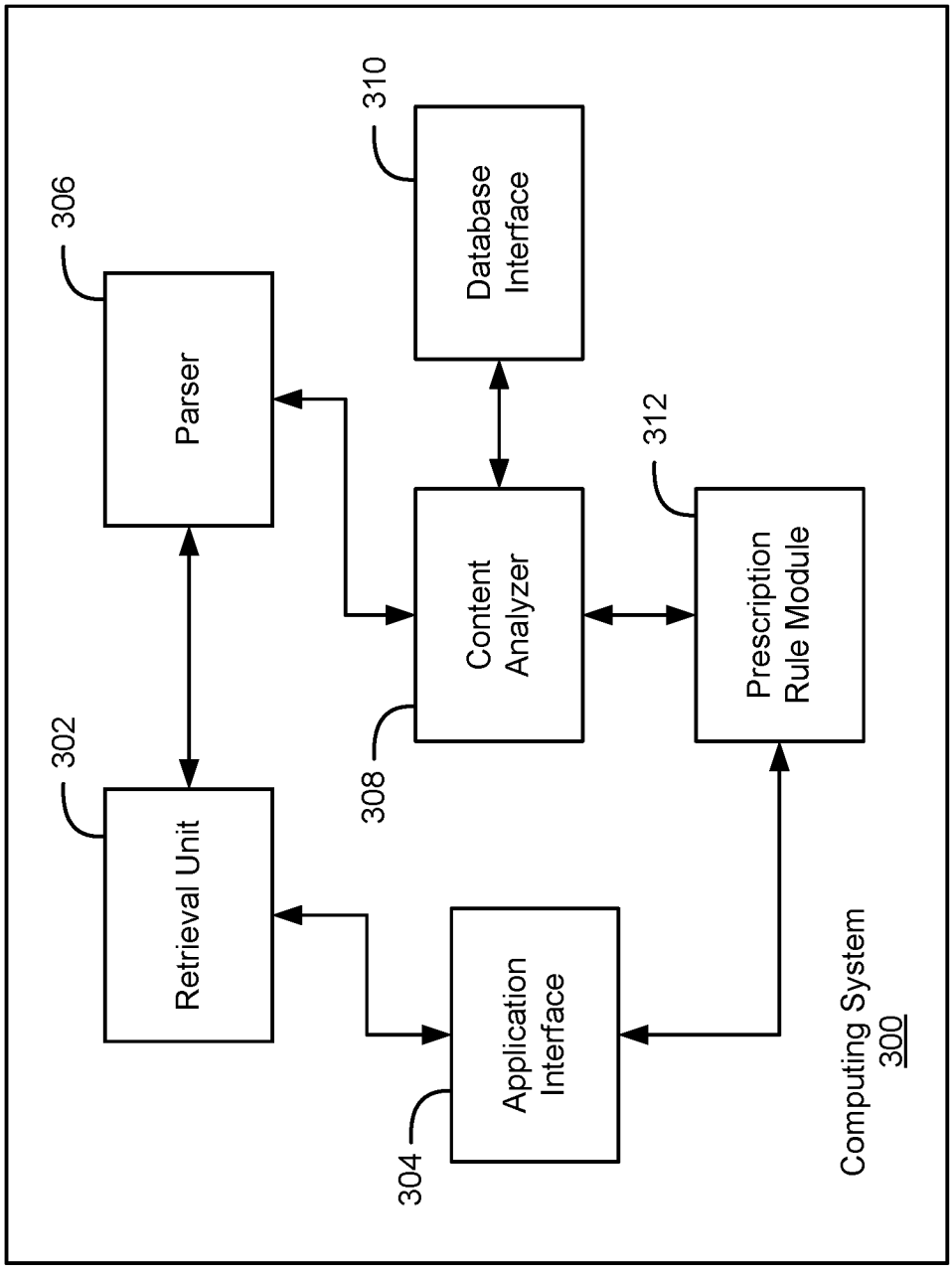
Computing System
300
Retrieval Unit
302
Application Interface
304
Content Analyzer
308
Parser
306
Database Interface
310
Prescription Rule Module
312

Fig. 3

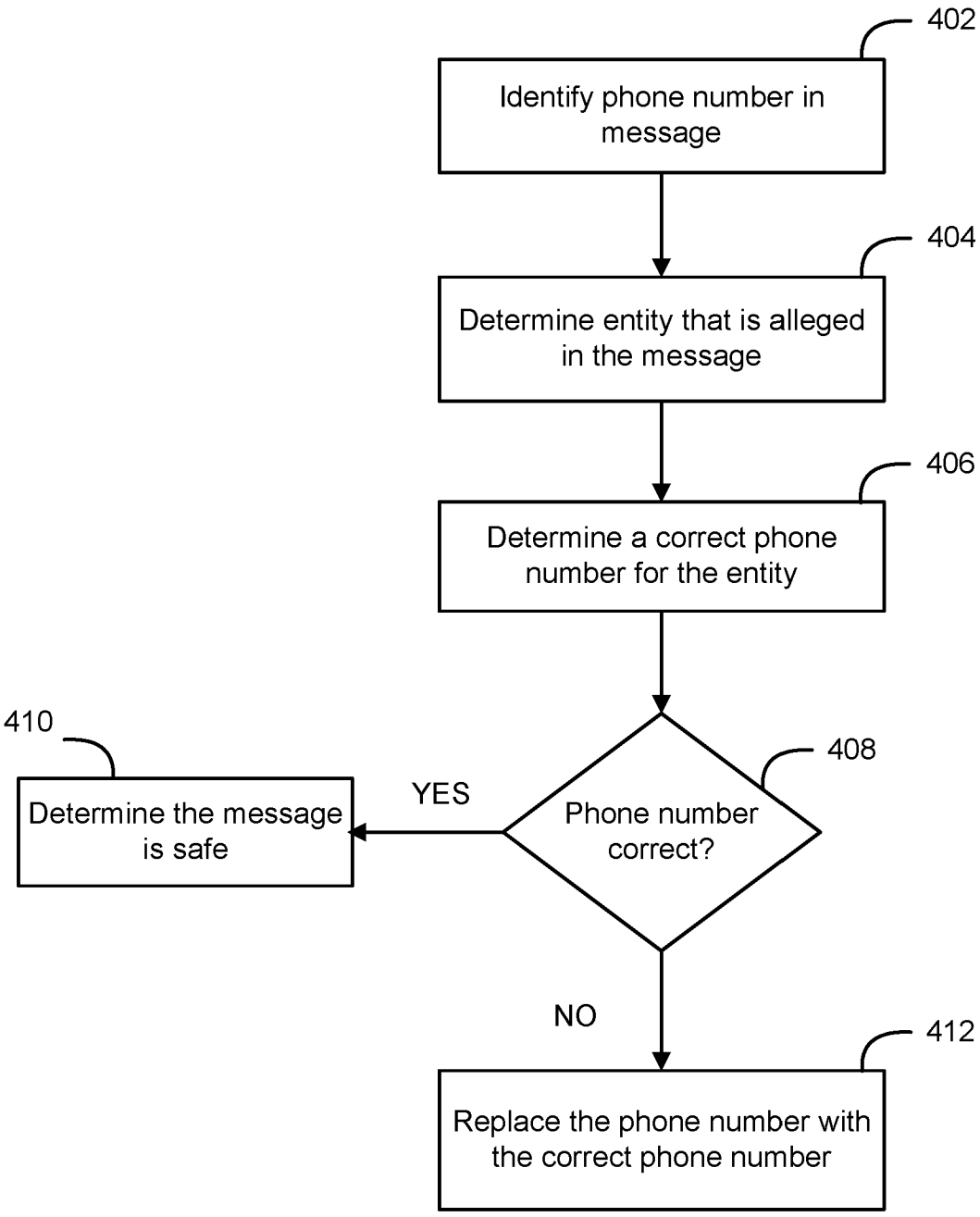
402
Identify phone number in message
404
Determine entity that is alleged in the message
406
Determine a correct phone number for the entity
408
Phone number correct?
YES
410
Determine the message is safe
NO
412
Replace the phone number with the correct phone number

Fig. 4

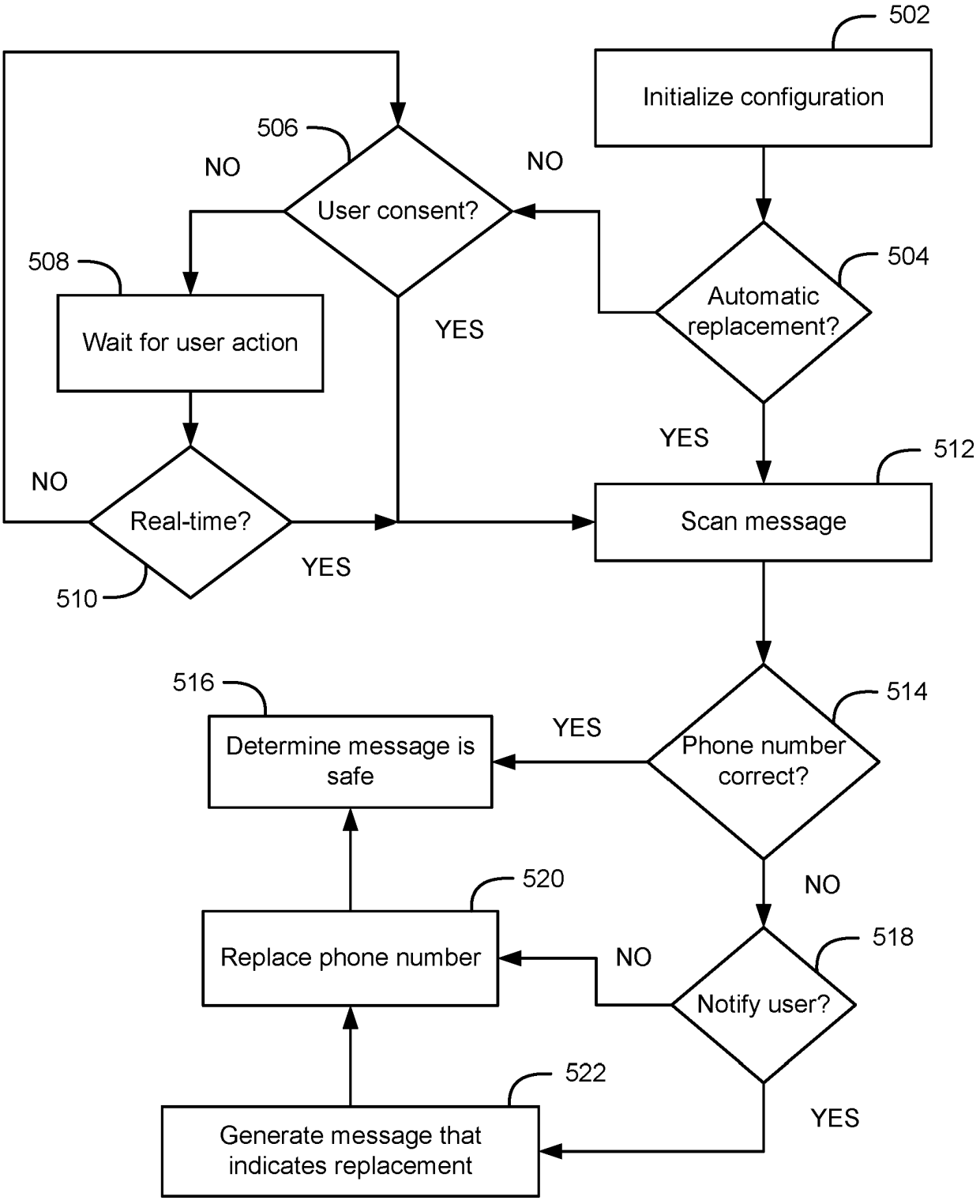
502
Initialize configuration
504
Automatic replacement?
NO
YES
506
User consent?
NO
YES
508
Wait for user action
510
Real-time?
NO
YES
512
Scan message
514
Phone number correct?
YES
516
Determine message is safe
NO
518
Notify user?
NO
YES
520
Replace phone number
522
Generate message that indicates replacement

Fig. 5

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2018249006 A **[0005]**
- US 10051121 B **[0016] [0027]**